Be Vigilant of Data Leaks Caused by the BlackCat Ransomware

Antiy CERT

Time of first release:3 July, 2023

This report is a machine-translated version.

1 Overview

Recently, Antiy CERT (member of the CCTGA Ransomware Prevention and Response Working Group) has found a number of BlackCat [1] ransomware attacks. Blackcat ransomware, also known as ALPHV or Noberus, was discovered in November 2021, with the attack organisation behind it operating based on the ransomware-as-a-service (RaaS) business model, releasing version 2.0 called "Sphynx" on February 21, 2023 [2], The initial access to the victim system is mainly realized through phishing, vulnerability utilization and the obtained credentials, and the system has the function of intranet propagation, and the data in the victim system will be stolen before the encryption payload is executed. The encryption payload uses AES or ChaCha combination of RSA algorithms to encrypt files, and no public decryption tools have been found.[1][2]

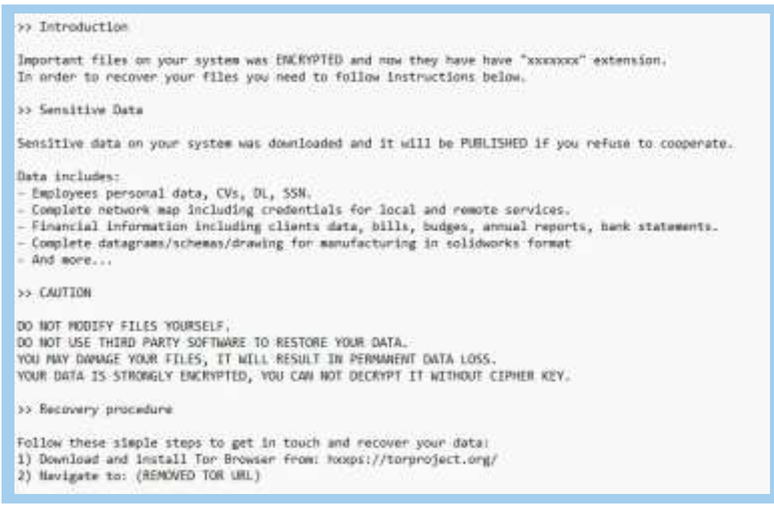
The attack organization behind the BlackCat ransomware adopts the double blackmail strategy of "stealing data + encrypted files," based on which the threat of harassment or DDoS attack is added to constitute multiple blackmail, and there is also the case of "no encryption only blackmail." It is one of the trends of the current ransomware attack organization to transform the pattern of ransomware. Compared with data encryption, the threat of data exposure will bring greater pressure to some of the victimized enterprises. As a result, some attack groups are beginning to add the ability to steal data to the ransomware while retaining its mechanism for encrypting files. The encrypted data may be recovered, and once it is leaked, the impact caused by the leakage is immeasurable, such as product formula, design drawings and cooperation agreement and other confidential documents. From November 30, 2021, the attack group behind the BlackCat ransomware has been publishing victim information and stolen data at the dedicated data breach site (DLS) of the Tor website, as of July 3, 2023. There are 434 victims in the DLS, and the actual number of victims far exceeds this number. this part is the information of the victims that is not satisfied with the needs of the victims or that is newly added, and the data that is stolen from the victim system. The attacker will remove the victim's information and stolen data when the demand is satisfied or for other reasons.

Blackcat ransomware is associated with REvil, DarkSide and BlackMatter ransomware that have exited the ransomware market [3], and is the first ransomware to develop cross-platform attack payloads using the Rust programming language [4]. Its payload supports execution on Windows, Linux, and VMware ESXi systems. Encryption of the payload needs to be performed by specific Access Token parameters, and the payload file cannot be executed without obtaining the Access Token parameters, in order to prevent security researchers and sandbox tools from analyzing the payload.[3][4]

Table 1-1 Overview of BlackCat ransomware 1

Family name	Blackcat (aka ALPHV or Noberus)
Time of occurrence	Nov-2021
Typical mode of transmission	Initial access is realized through phishing, vulnerability exploitation and acquired credentials, and it has the function of intranet propagation
Typical Encryption Suffix	. (Random combination of 6-7 digits + letters)
Encryption algorithm	Aes or ChaCha + RSA
Decryption tools	No public decryption tools have been found
Encryption system	Windows, Linux and VMware ESXi
Double blackmail or not	Yes

Ransom note



```
>> Introduction

Important files on your system was ENCRYPTED and now they have have "xxxxxxx" extension.
In order to recover your files you need to follow instructions below.

>> Sensitive Data

Sensitive data on your system was downloaded and it will be PUBLISHED if you refuse to cooperate.

Data includes:
- Employees personal data, CVs, DL, SSN.
- Complete network map including credentials for local and remote services.
- Financial information including clients data, bills, budges, annual reports, bank statements.
- Complete datagrams/schemas/drawing for manufacturing in solidworks format
- And more...

>> CAUTION

DO NOT MODIFY FILES YOURSELF.
DO NOT USE THIRD PARTY SOFTWARE TO RESTORE YOUR DATA.
YOU MAY DAMAGE YOUR FILES, IT WILL RESULT IN PERMANENT DATA LOSS.
YOUR DATA IS STRONGLY ENCRYPTED, YOU CAN NOT DECRYPT IT WITHOUT CIPHER KEY.

>> Recovery procedure

Follow these simple steps to get in touch and recover your data:
1) Download and install Tor Browser from: hxxps://torproject.org/
2) Navigate to: (REMOVED TOR URL)
```

It is proved that Antiy IEP can effectively detect and kill the ransomware.

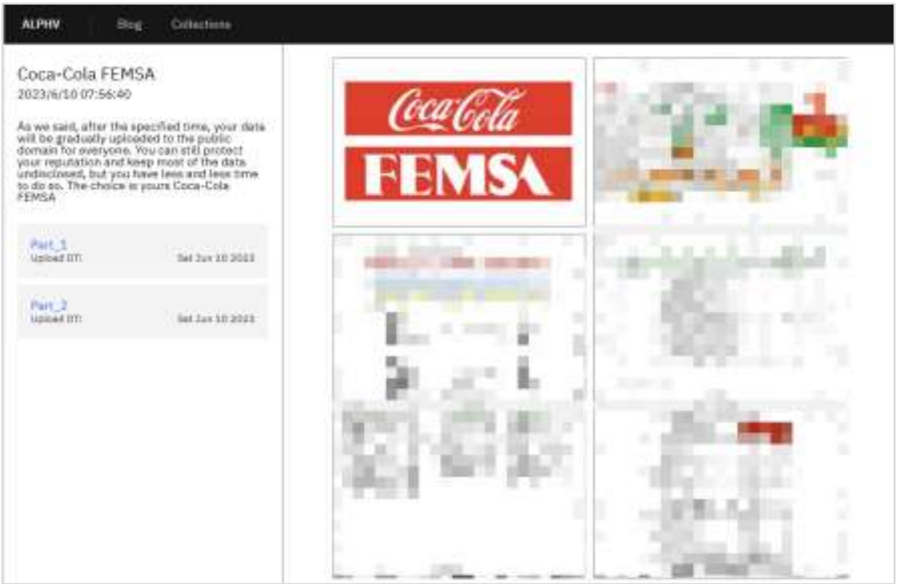
2 Recent data leakage cases

From November 30, 2021, the attack group behind the BlackCat ransomware has been publishing victim information and stolen data at the dedicated data breach site (DLS) of the Tor website, as of July 3, 2023. There are 434 victims in their DLS.

The following are some of the victims and data breaches released by the group behind the BlackCat ransomware attack.

2.1 Mexican beverage company Coca-Cola FEMSA

The attackers updated the Mexican beverage company Coca-Cola FEMSA located in their DLS on June 10, 2023. The attacker has disclosed two parts of data, Part _ 1 and Part _ 2, and the contents of the sample pictures are the order information, transaction contract and profit sharing contract between Coca-Cola FEMSA company and its partner company.



Coca-Cola FEMSA
2023/6/10 07:56:40

As we said, after the specified time, your data will be gradually uploaded to the public domain for everyone. You can still protect your reputation and keep most of the data undisclosed, but you have less and less time to do so. The choice is yours Coca-Cola FEMSA

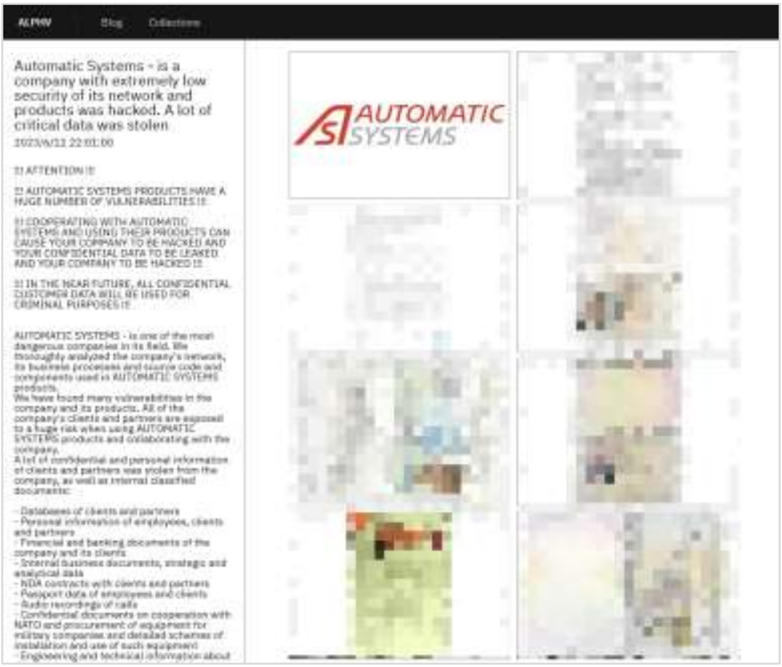
Part_1
Upload DT: Sat Jun 10 2023

Part_2
Upload DT: Sat Jun 10 2023

Figure 2-1 Victim Coca-Cola FEMSA Information 1

2.2 Automatic systems, a Belgian company that manufactures access control equipment

On June 12, the attackers updated information on Automatic Systems, a Belgian company that manufactures access control equipment located in their DLS. The documents the attackers claimed to have stolen include but are not limited to personal information of Automatic Systems employees and customers, drawings of product designs and business data, as well as documents such as agreements and plans signed with NATO. The contents of the sample pictures are the personal identification information of the employees of Automatic Systems, the order information of the cooperative company, the contract and the confidentiality agreement and other documents.



Automatic Systems - is a company with extremely low security of its network and products was hacked. A lot of critical data was stolen

2023/6/12 22:01:00

!! ATTENTION !!

!! AUTOMATIC SYSTEMS PRODUCTS HAVE A HUGE NUMBER OF VULNERABILITIES !!

!! COOPERATING WITH AUTOMATIC SYSTEMS AND USING THEIR PRODUCTS CAN CAUSE YOUR COMPANY TO BE HACKED AND YOUR CONFIDENTIAL DATA TO BE LEAKED AND YOUR COMPANY TO BE HACKED !!

!! IN THE NEAR FUTURE, ALL CONFIDENTIAL CUSTOMER DATA WILL BE USED FOR CRIMINAL PURPOSES !!

AUTOMATIC SYSTEMS - is one of the most dangerous companies in its field. We thoroughly analyzed the company's network, its business processes and source code and components used in AUTOMATIC SYSTEMS products.
We have found many vulnerabilities in the company and its products. All of the company's clients and partners are exposed to a huge risk when using AUTOMATIC SYSTEMS products and collaborating with the company.
A lot of confidential and personal information of clients and partners was stolen from the company, as well as internal classified documents:

- Databases of clients and partners
- Personal information of employees, clients and partners
- Financial and banking documents of the company and its clients
- Internal business documents, strategic and analytical data
- NDA contracts with clients and partners
- Passport data of employees and clients
- Audio recordings of calls
- Confidential documents on cooperation with NATO and procurement of equipment for military companies and detailed schemes of installation and use of such equipment
- Engineering and technical information about

Figure 2-2 Victim automatic systems information2

Where documents of confidentiality agreement with Alibaba were found.

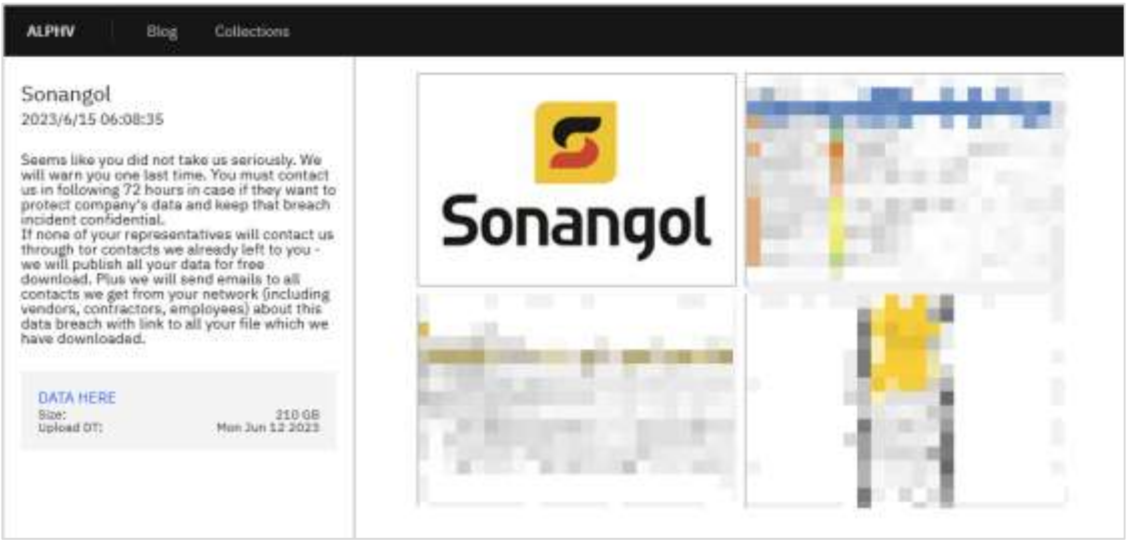
2021-Alibaba-NDA-v4-bd-18june

Figure 2-3 Relevant documents about Alibaba3

2.3 State oil company Sonangol of the Republic of Angola

On 15 June, the attackers updated information relating to Sonangol, the national oil company of the Republic of Angola, which is located in its DLS, as well as 210 gigabytes of data stolen from the company, This includes information on Sonangol's employees, financial documents and medical systems.

The attacker warned the victim "to contact him within 72 hours, to release all data if overdue, and to send e-mails to all concerned about the data breach. Including suppliers, contractors and employees. "



Sonangol

2023/6/15 06:08:35

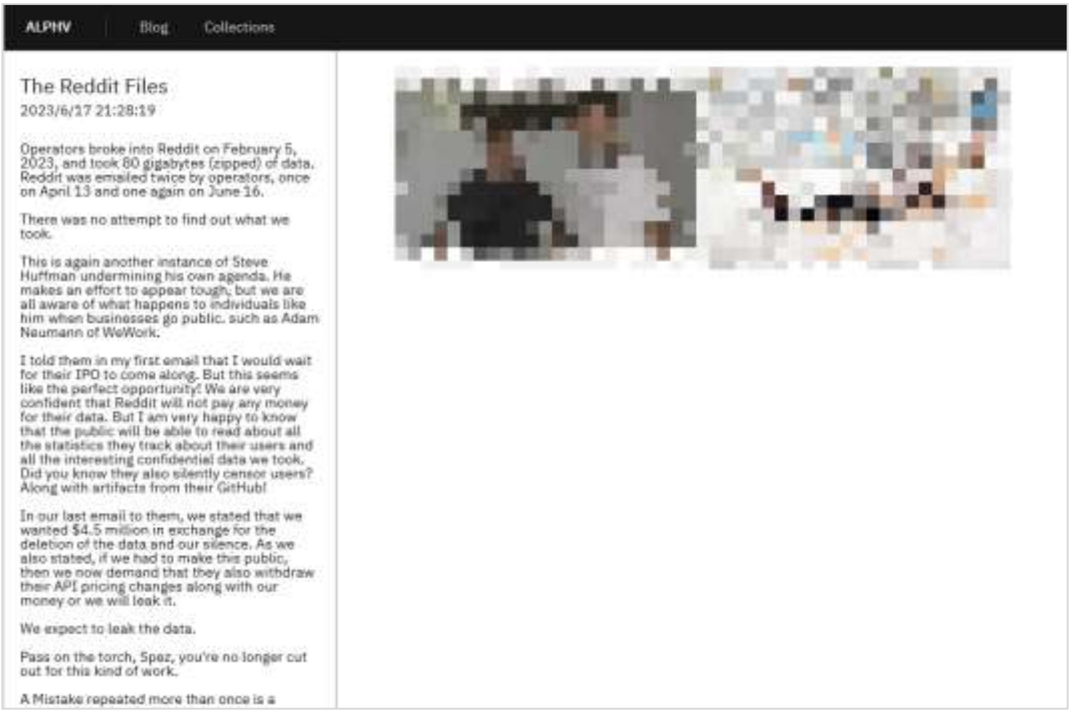
Seems like you did not take us seriously. We will warn you one last time. You must contact us in following 72 hours in case if they want to protect company's data and keep that breach incident confidential.
If none of your representatives will contact us through tor contacts we already left to you - we will publish all your data for free download. Plus we will send emails to all contacts we get from your network (including vendors, contractors, employees) about this data breach with link to all your file which we have downloaded.

DATA HERE
Size: 210 GB
Upload DT: Mon Jun 12 2023

Figure 2-4 Information on victim Sonangol

2.4 US social news site Reddit

On June 17, the attackers updated information about Reddit, the US social news site that was placed on their DLS site. The attackers claimed to have hacked into Reddit's systems on February 5, 2023, after Reddit employees were subjected to a targeted phishing attack [5] in which the attackers stole 80GB of compressed data, And sent two emails to Reddit, on April 13 and June 16, but received no response. The attackers wanted $4.5 million as a ransom and demanded that Reddit retract their recent decision to raise API pricing.[5]



The Reddit Files

2023/6/17 21:28:19

Operators broke into Reddit on February 5, 2023, and took 80 gigabytes (zipped) of data. Reddit was emailed twice by operators, once on April 13 and one again on June 16.

There was no attempt to find out what we took.

This is again another instance of Steve Huffman undermining his own agenda. He makes an effort to appear tough, but we are all aware of what happens to individuals like him when businesses go public. such as Adam Neumann of WeWork.

I told them in my first email that I would wait for their IPO to come along. But this seems like the perfect opportunity! We are very confident that Reddit will not pay any money for their data. But I am very happy to know that the public will be able to read about all the statistics they track about their users and all the interesting confidential data we took. Did you know they also silently censor users? Along with artifacts from their GitHub!

In our last email to them, we stated that we wanted $4.5 million in exchange for the deletion of the data and our silence. As we also stated, if we had to make this public, then we now demand that they also withdraw their API pricing changes along with our money or we will leak it.

We expect to leak the data.

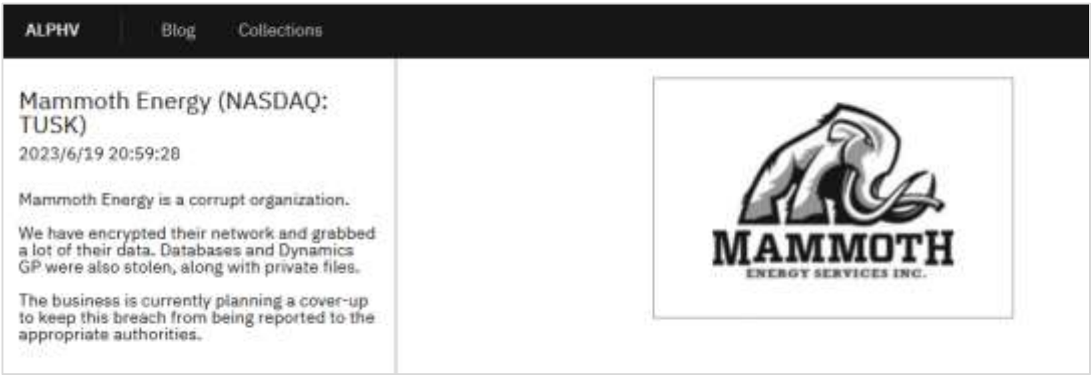
Pass on the torch, Spez, you're no longer cut out for this kind of work.

A Mistake repeated more than once is a

Figure 2-5 Victim Reddit messages 4

2.5 Mammoth Energy, an American energy services company

On June 19, the attackers updated information related to Mammoth Energy, an American energy service company located in its DLS, claiming that they had encrypted the company's network facilities and had stolen a large amount of data from inside the company, Including database files, Dynamics GP files and private files.



Mammoth Energy (NASDAQ: TUSK)

2023/6/19 20:59:28

Mammoth Energy is a corrupt organization.

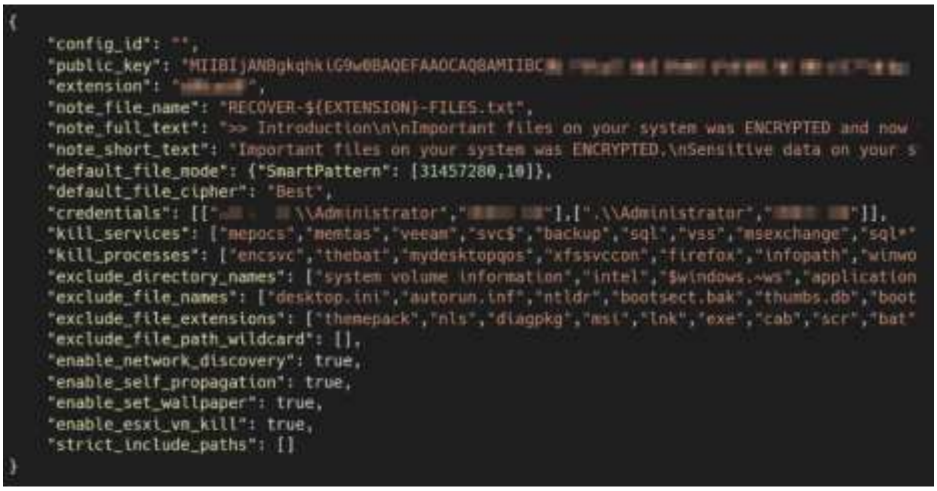
We have encrypted their network and grabbed a lot of their data. Databases and Dynamics GP were also stolen, along with private files.

The business is currently planning a cover-up to keep this breach from being reported to the appropriate authorities.

Figure 2-6 Victim Mammoth Energy Information

3 Sorting of Load Function and Technology

The BlackCat ransomware payload is written in the Rust programming language, and the execution payload requires a specific Access Token parameter to decrypt the encrypted configuration file written to the ransomware payload file. The configuration file is the content of a file set according to the actual situation of the victim system after the attacker intrudes the victim system, and the configuration file includes a list of services and processes to be stopped. Skip encrypted white list directories, files, and list of file extensions. The load file cannot be executed without access to the Access Token parameter in order to prevent the security researcher and sandbox tool from analyzing the load.



```
{
    "config_id": "",
    "public_key": "MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBC[redacted]
    "extension": "[redacted]",
    "note_file_name": "RECOVER-${EXTENSION}-FILES.txt",
    "note_full_text": ">> Introduction\n\nImportant files on your system was ENCRYPTED and now
    "note_short_text": "Important files on your system was ENCRYPTED.\nSensitive data on your s
    "default_file_mode": {"SmartPattern": [31457280,10]},
    "default_file_cipher": "Best",
    "credentials": [["[redacted]\\Administrator","[redacted]"],[".\\Administrator","[redacted]"]],
    "kill_services": ["mepocs","memtas","veeam","svc$","backup","sql","vss","msexchange","sql*"
    "kill_processes": ["encsvc","thebat","mydesktopqos","xfssvccon","firefox","infopath","winwo
    "exclude_directory_names": ["system volume information","intel","$windows.~ws","application
    "exclude_file_names": ["desktop.ini","autorun.inf","ntldr","bootsect.bak","thumbs.db","boot
    "exclude_file_extensions": ["themepack","nls","diagpkg","msi","lnk","exe","cab","scr","bat"
    "exclude_file_path_wildcard": [],
    "enable_network_discovery": true,
    "enable_self_propagation": true,
    "enable_set_wallpaper": true,
    "enable_esxi_vm_kill": true,
    "strict_include_paths": []
}
```

Figure 3-1 Content of configuration file 1

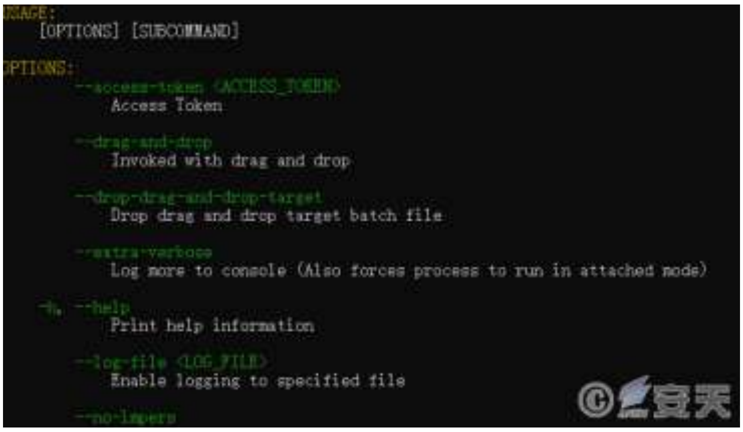
The following is a brief description of the options included in the configuration file.

Table 3-1 Configuration file options and brief description 1

Configuration options	Description	Configuration options	Description
Config _ id	Id information	Kill _ processes	End a particular process
Public _ key	Rsa public key	Include _ directory _ names	Bypass the encrypted file directory
Extension	Suffix (combination of letters and numbers)	Include _ file _ names	Bypass the encrypted file name
Note _ file _ name	Name of the ransom note file	Include _ file _ extensions	Bypass the encrypted file suffix
Note _ full _ text	Full text of the ransom note	Include _ file _ path _ wildcard	Bypass the encrypted file path

Note _ short _ text	A short ransom note for desktop backgrounds	Enable _ network _ discovery	Discover other hosts in the network environment
Default _ file _ mode	File Encryption Mode	Enable _ self _ propagation	Self-transmission model
Default _ file _ cipher	Using a specific encryption algorithm	Enable _ set _ wallpaper	Modify desktop wallpaper
Credentials	Specific Voucher Information of Victim	Enable _ esxi _ vm _ kill	Terminate VMware ESXi
Kill _ services	End a specific service	Strict _ include _ paths	Specify a path

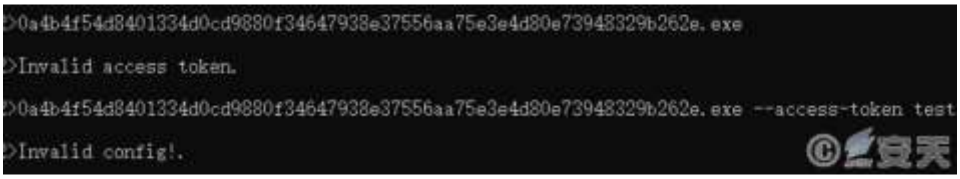
Blackcat ransomware payload execution needs to pass specific parameters.



```
USAGE:
    [OPTIONS] [SUBCOMMAND]

OPTIONS:
        --access-token <ACCESS_TOKEN>
            Access Token

        --drag-and-drop
            Invoked with drag and drop

        --drop-drag-and-drop-target
            Drop drag and drop target batch file

        --extra-verbose
            Log more to console (Also forces process to run in attached mode)

    -h, --help
            Print help information

        --log-file <LOG_FILE>
            Enable logging to specified file

        --no-impers
```

Figure 3-2 Execution of loads by parameters 2

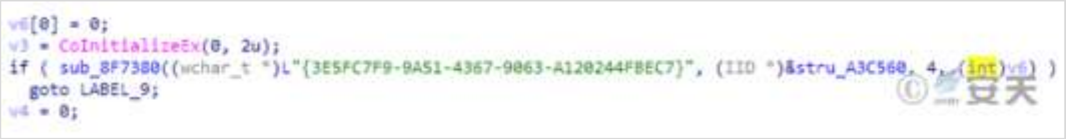
The Access Token parameter is the key to decrypt the built-in configuration information of the payload, and if the parameter is incorrect, the payload cannot be executed, so as to avoid the detection of automatic analysis systems such as sandboxes and the extraction of configuration information.



```
>0a4b4f54d8401334d0cd9880f34647938e37556aa75e3e4d80e73948329b262e.exe

>Invalid access token.

>0a4b4f54d8401334d0cd9880f34647938e37556aa75e3e4d80e73948329b262e.exe --access-token test

>Invalid config!.
```

Figure 3-3 Decrypting the configuration file with the Access Token3

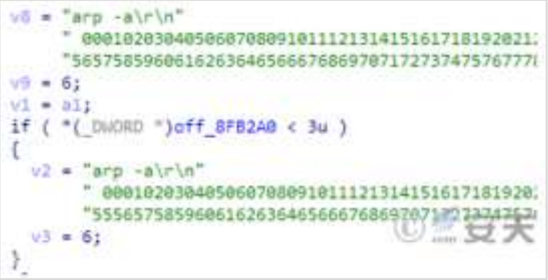
Use COM API to bypass user account control (UAC), so as to achieve the right.



```
v6[0] = 0;
v3 = CoInitializeEx(0, 2u);
if ( sub_8F7380((wchar_t *)L"{3E5FC7F9-9A51-4367-9063-A120244FBEC7}", (IID *)&stru_A3C560, 4, (int)v6) )
  goto LABEL_9;
v4 = 0;
```

Figure 3-4 Using COM to extract weights4

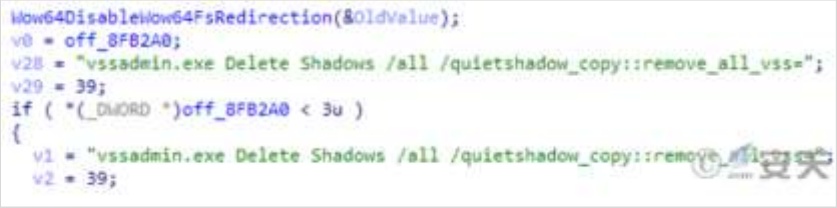
Check the ARP cache information of the victim system, and obtain the resolved IP address and the corresponding MAC address on the current computer.



```
v8 = "arp -a\r\n"
     " 000102030405060708091011121314151617181920211
     "5657585960616263646566676869707172737475767778
v9 = 6;
v1 = a1;
if ( *(_DWORD *)off_8FB2A0 < 3u )
{
  v2 = "arp -a\r\n"
       " 00010203040506070809101112131415161718192021
       "555657585960616263646566676869707172737475
  v3 = 6;
}
```

Figure 3-5 Obtaining ARP information 5

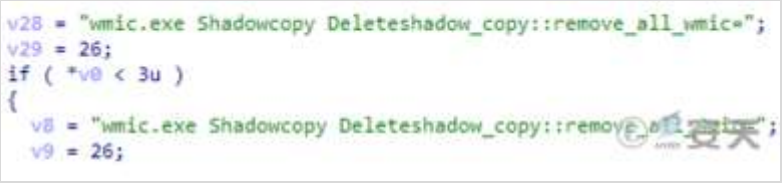
Use vssadmin. exe to delete shadow copies to prevent users from restoring encrypted files by restoring shadow.



```
Wow64DisableWow64FsRedirection(&OldValue);
v0 = off_8FB2A0;
v28 = "vssadmin.exe Delete Shadows /all /quietshadow_copy::remove_all_vss=";
v29 = 39;
if ( *(_DWORD *)off_8FB2A0 < 3u )
{
  v1 = "vssadmin.exe Delete Shadows /all /quietshadow_copy::remove_all_vss=";
  v2 = 39;
```

Figure 3-6 Removing shadow copies using vssadmin. exe6

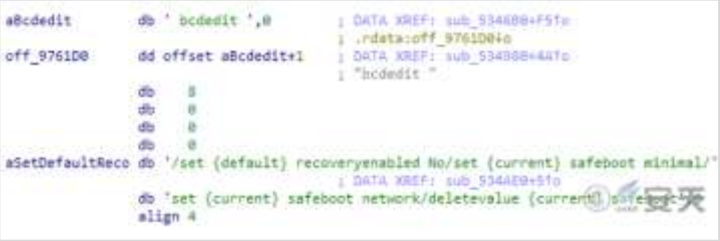
Use wmic .exe to delete shadow copies to prevent users from restoring encrypted files by restoring shadow.



```
v28 = "wmic.exe Shadowcopy Deleteshadow_copy::remove_all_wmic=";
v29 = 26;
if ( *v0 < 3u )
{
  v8 = "wmic.exe Shadowcopy Deleteshadow_copy::remove_all_wmic=";
  v9 = 26;
```

Figure 3-7 Removing shadow copies using wmic .exe 7

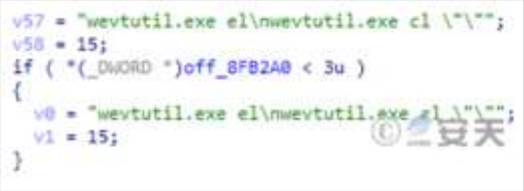
Disable automatic system recovery with bcdedit and set to start in secure mode with network support.



```
aBcdedit         db ' bcdedit ',0         ; DATA XREF: sub_534680+F5↑o
                                          ; .rdata:off_9761D0↓o
off_9761D0       dd offset aBcdedit+1     ; DATA XREF: sub_534B80+4A↑o
                                          ; "bcdedit "
                 db    5
                 db    0
                 db    0
                 db    0
aSetDefaultReco  db '/set {default} recoveryenabled No/set {current} safeboot minimal/'
                                          ; DATA XREF: sub_534AE0+51o
                 db 'set {current} safeboot network/deletevalue {current} safeboot'
                 align 4
```

Figure 3-8 Disable repair and starting in safe mode 8

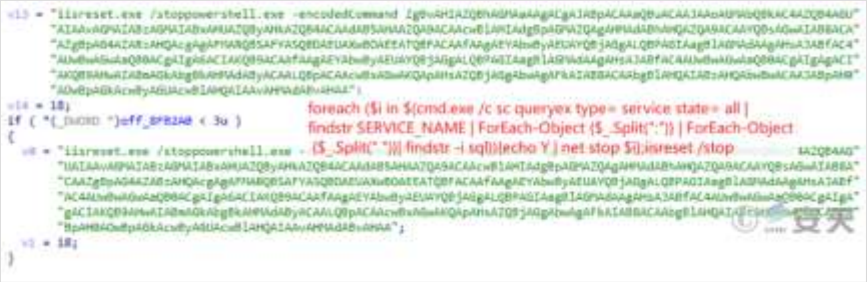
Call wevtutil.exe to clear the log, so as to prevent the user from finding relevant information of intrusion through the log.



```
v57 = "wevtutil.exe el\nwevtutil.exe cl \"\"";
v58 = 15;
if ( *(_DWORD *)off_8FB2A0 < 3u )
{
  v0 = "wevtutil.exe el\nwevtutil.exe cl \"\"";
  v1 = 15;
}
```

Figure 3-9 Clearing log 9

End the service specified in the configuration file to prevent the execution of the ransomware payload from being affected.

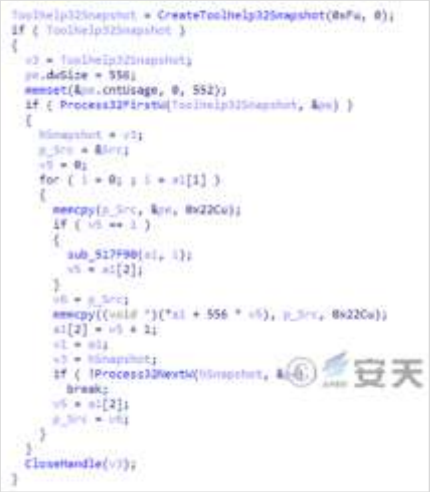


```
v13 = "iisreset.exe /stoppowershell.exe -encodedCommand [illegible]"
      "[illegible]"
      "[illegible]"
      "[illegible]"
      "[illegible]"
      "[illegible]";
v14 = 18;
if ( *(_DWORD *)off_8FB2A0 < 3u )
{
  v0 = "iisreset.exe /stoppowershell.exe [illegible]"
       "[illegible]"
       "[illegible]"
       "[illegible]"
       "[illegible]"
       "[illegible]";
  v1 = 18;
}
```

foreach ($i in $(cmd.exe /c sc queryex type= service state= all | findstr SERVICE_NAME | ForEach-Object {$_.Split(":")} | ForEach-Object {$_.Split(" ")}| findstr -i sql)){echo Y | net stop $i};isreset /stop

Figure 3-10 End a particular service 10

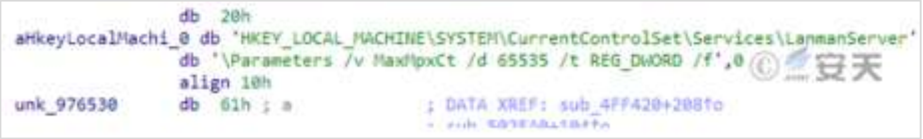
Ends the process specified in the configuration file to prevent the execution of the ransomware payload from being affected.



```
Toolhelp32Snapshot = CreateToolhelp32Snapshot(0xFu, 0);
if ( Toolhelp32Snapshot )
{
  v3 = Toolhelp32Snapshot;
  pe.dwSize = 556;
  memset(&pe.cntUsage, 0, 552);
  if ( Process32FirstW(Toolhelp32Snapshot, &pe) )
  {
    hSnapshot = v3;
    p_Src = &Src;
    v5 = 0;
    for ( i = 0; ; i = a1[1] )
    {
      memcpy(p_Src, &pe, 0x22Cu);
      if ( v5 == i )
      {
        sub_517F90(a1, i);
        v5 = a1[2];
      }
      v6 = p_Src;
      memcpy((void *)(*a1 + 556 * v5), p_Src, 0x22Cu);
      a1[2] = v5 + 1;
      v1 = a1;
      v3 = hSnapshot;
      if ( !Process32NextW(hSnapshot, &pe) )
        break;
      v5 = a1[2];
      p_Src = v6;
    }
  }
  CloseHandle(v3);
}
```

Figure 3-11 End a particular process 11

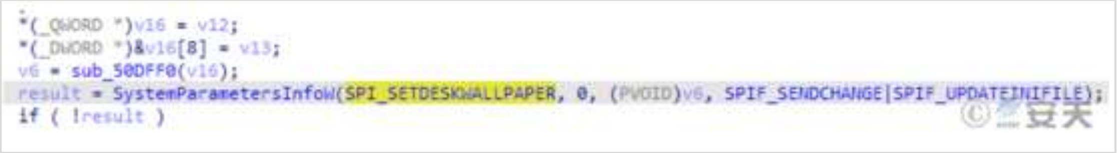
Services are created in the victim system to implement persistence.



```
                  db  20h
aHkeyLocalMachi_0 db 'HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer'
                  db '\Parameters /v MaxMpxCt /d 65535 /t REG_DWORD /f',0
                  align 10h
unk_976530        db  61h ; a                ; DATA XREF: sub_4FF420+208fo
```

Diagram 3-12 Creating a service implementation persistence 12

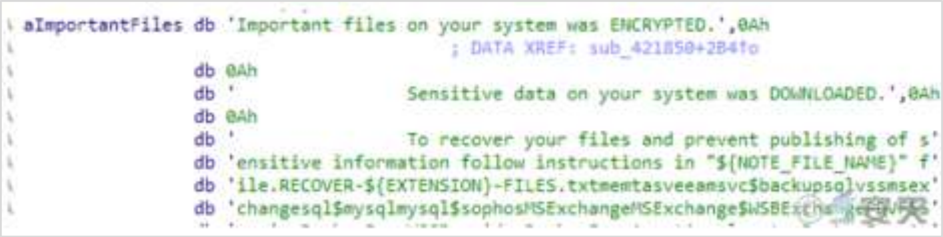
Sets a specific image with a blackmail alert as a desktop background file.



```
*(_QWORD *)v16 = v12;
*(_DWORD *)&v16[8] = v13;
v6 = sub_50DFF0(v16);
result = SystemParametersInfoW(SPI_SETDESKWALLPAPER, 0, (PVOID)v6, SPIF_SENDCHANGE|SPIF_UPDATEINIFILE);
if ( !result )
```

Figure 3-13 Modifying Desktop Background13

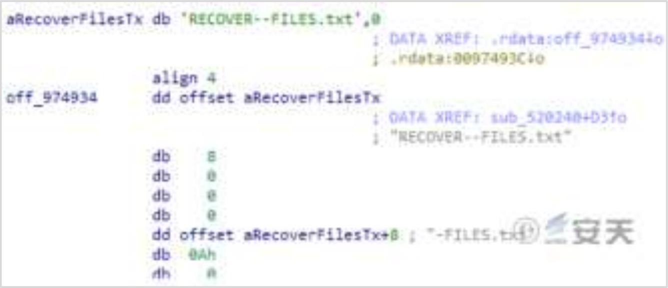
Concatenates a specific string in the code into the content of the ransom note.



```
aImportantFiles db 'Important files on your system was ENCRYPTED.',0Ah
                                        ; DATA XREF: sub_421850+2B4fo
                db 0Ah
                db '                    Sensitive data on your system was DOWNLOADED.',0Ah
                db 0Ah
                db '                    To recover your files and prevent publishing of s'
                db 'ensitive information follow instructions in "${NOTE_FILE_NAME}" f'
                db 'ile.RECOVER-${EXTENSION}-FILES.txtmemtasveeamsvc$backupsqlvssmsex'
                db 'changesql$mysqlmysql$sophosMSExchangeMSExchange$WSBExchange'
```

Figure 3-14 Splicing the contents of the ransom note14

Generates a blackmail letter named "RECOVER- (suffix set in the configuration file) - FILES. txt," such as "RECOVER- locked - FILES. txt."



```
aRecoverFilesTx db 'RECOVER--FILES.txt',0
                                        ; DATA XREF: .rdata:off_974934↓o
                                        ; .rdata:0097493C↓o
                align 4
off_974934      dd offset aRecoverFilesTx
                                        ; DATA XREF: sub_520240+D3fo
                                        ; "RECOVER--FILES.txt"
                db    8
                db    0
                db    0
                db    0
                dd offset aRecoverFilesTx+8 ; "-FILES.txt"
                db  0Ah
                db    0
```

Figure 3-15 Setting the name of a blackmail letter 15

4 Recommendations for protection

In response to ransomware attacks, Antiy recommends that individuals and businesses take the following precautions:

4.1 Personal protection

1. Enhance network security awareness: Maintain good habits of network use and actively learn relevant knowledge of network security;
2. Install terminal protection: Install anti-virus software. It is suggested that Antiy IEP users open the ransomware defense tool module (open by default);
3. Strengthen password strength: Avoid using weak passwords, recommend using 16-digit or longer passwords, including combinations of upper and lower case letters, numbers and symbols, and avoid using the same password for multiple servers;
4. Change passwords on a regular basis: Change system passwords on a regular basis to avoid system intrusion due to password leakage;
5. Update patches in time: It is suggested to open automatic update and install system patches, and update system patches in time for vulnerable parts such as servers, databases and middleware;
6. Close high-risk ports: The principle of minimizing external services is to close unused high-risk ports such as 135, 139, 445 and 3389;
7. Close PowerShell: If PowerShell command line tools are not used, it is recommended to close them;
8. Regular data backup: Data backup of important files on a regular basis, and backup data shall be isolated from the host computer.

4.2 Enterprise protection

1. Network security training and security drill: Regularly carry out network security training and security drill to improve employees "network security awareness;
2. Install terminal protection: Install anti-virus software, and recommend the installation of Antiy IEP for different platforms;
3. Update patches in time: It is suggested to open automatic update and install system patches, and update system patches in time for vulnerable parts such as servers, databases and middleware;

4. Enable log: Enable the key log collection function (security log, system log, PowerShell log, IIS log, error log, access log, transmission log and cookie log) to provide a foundation for security event tracing and tracing;

5. Set IP whitelist rules: Configure advanced secure Windows firewall, set the inbound rules for remote desktop connection, add the IP address or IP address range used to the rules, and prevent violent attack of non-rule IPs;

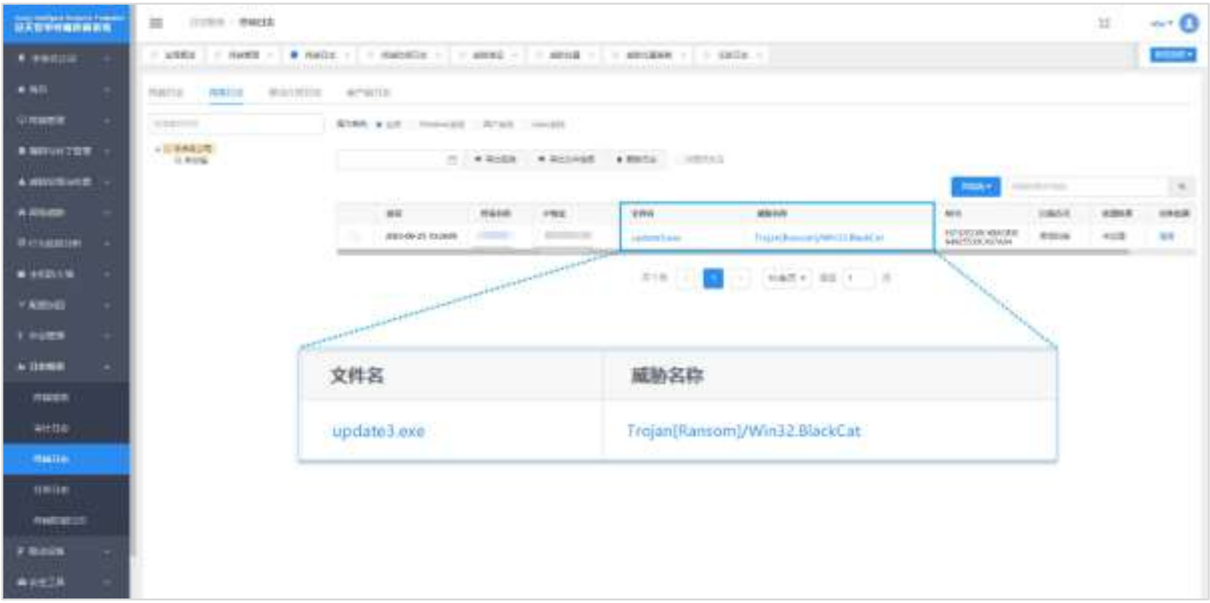
6. Host reinforcement: Conduct penetration test and safety reinforcement for the system;

7. Deploy Intrusion Detection System (IDS): Deploy traffic monitoring software or equipment to facilitate the discovery, tracing and tracing of ransomware. Taking network traffic as the detection and analysis object, the Antiy PTD can accurately detect a mass of known malicious codes and network attack activities, and effectively detect suspicious behaviors, assets and various unknown threats on the network;

8. Disaster backup plan: Establish a security disaster backup plan to ensure that the backup business system can be quickly enabled in case of a security event;

9. Safe service: In case of a ransomware attack, it is recommended to disconnect the network in time, and protect the site and wait for the security engineer to check the computer. Antiy 7 * 24 Service Hotline: 400-840-9234.

It is proved that Antiy IEP can effectively detect and kill the ransomware.



文件名	威胁名称
update3.exe	Trojan[Ransom]/Win32.BlackCat

Figure 4-1 Antiy IEP can effectively detect and kill the ransomware 1

5 ATT&CK Mapping graph of event

The technical characteristics corresponding to the event are shown in the figure below.

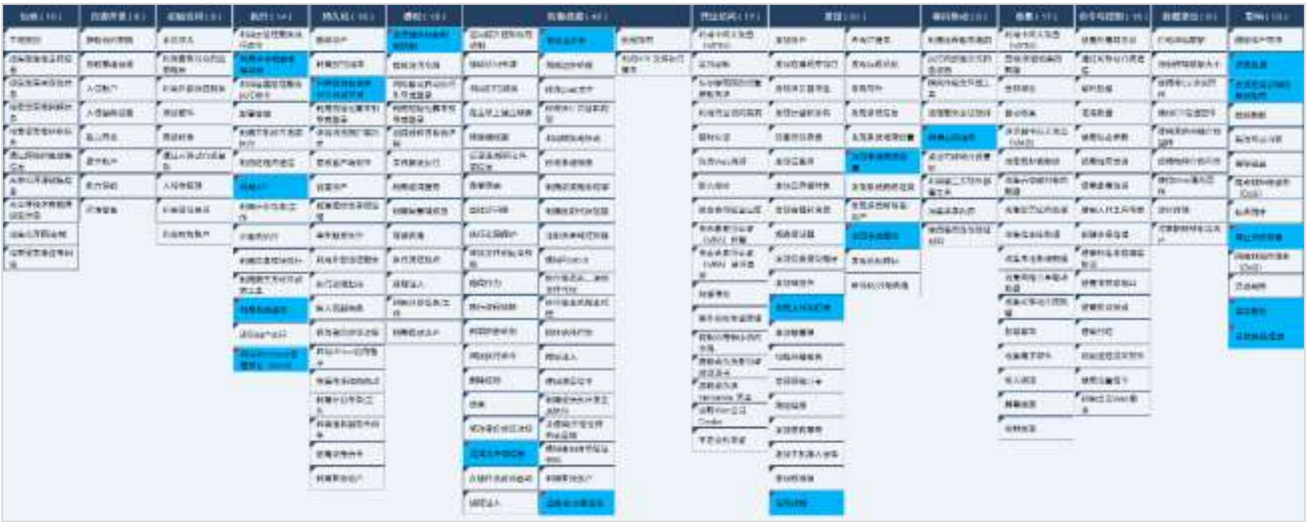


Figure 5-1 Mapping of Technical Features to ATT&CK1

Specific ATT&CK technical behavior description table is as follows.

Table 5-1 ATT&CK Technical Behavior Description Table 1

ATT&CK stages / categories	Specific behavior	Notes
Execution	Using command and script interpreters	The load is executed using commands and specified parameters
	Use API	Using COM API to Exert Power
	Utilization of system services	Execute the load using the system service
	Using Windows Management Specification (WMI)	Use wmic to execute command to delete shadow
Persistence	Use automatic startup to perform booting or logging	Achieve persistence by creating a service
Right to Submission	Abuse of enhanced control authority mechanism	Using COM API to Bypass UAC
Defensive evasion	Confusion of documents or information	Obfuscate part of a code segment
	Modify the registry	Create a registry key implementation to run as a service
	Virtualization / Sandbox Escape	Parameter execution to avoid sandbox analysis

Findings	Find files and directories	Find encrypted / bypassed files and directories
	Discovery Process	Discover the process to achieve an end process
	Discovery system network configuration	Discover network configuration by ARP command
	Discovery of system services	Discovery of system services to achieve end-of-service
Lateral movement	Use remote services	Using Remote Service to Realize Horizontal Movement
Impact	Damage data	Delete system log
	Data encryption with adverse effects	To encrypt a particular file
	Disable system recovery	Disable system recovery to avoid data recovery
	Disable the service	Stopping a particular service avoids interfering with the encryption
	System shutdown / restart	Restart the system in safe mode

6 Iocs

Md5
E6732e23b16b8cb5ea4925539c437a04
6ff9900b271090361e63f5242ee4e8b0
2891ec6365b7b0ef90899a35e4f2f747
B00b5eb046fe27f645b2a9b7aecc0205
8f2b7a45a93ee6f4806918aaa99c1b1b
B67ffe5e49ada7628ae9c32eaa3b4ce3
Ee159afcadc7eb4ba73f72c2f6924da3

Appendix I: Reference

[1]. Popular ransomware inventory by 2022

Https: / / www.antiy.cn / research / notice & report / research _ report / 20230130.html

[2]. Alphv ransomware group formulated their dependencies of a new'product'update.

Https: / / twitter.com / vxunderground / status / 1649094229413761030

[3]. Blackcat Ransomware (ALPHV)

Https: / / www.varonis.com / blog / blackcat-ransomware

[4]. Fbi Releases IOCs Associated with BlackCat / ALPHV Ransomware

Https: / / www.cisa.gov / news-events / alerts / 2022 / 04 / 22 / fbi-releases-iocs-associated-blackcatalog-ransomware

[5]. We had a security incident.Here's what we know.

Https: / / www.reddit.com / r / reddit / comments / 10y427y / we _ had _ a _ security _ incident _ where _ what _ we _ know /

Appendix II: About Antiy

Antiy is committed to enhancing the network security defense capabilities of its customers and effectively responding to security threats. Through more than 20 years of independent research and development, Antiy has developed technological leadership in areas such as threat detection engines, advanced threat countermeasures, and large-scale threat automation analysis.

Antiy has developed IEP (Intelligent Endpoint Protection System) security product family for PC, server and other system environments, as well as UWP (Unified Workload Protect) security products for cloud hosts, container and other system environments, providing system security capabilities including endpoint antivirus, endpoint protection (EPP), endpoint detection and response (EDR), and Cloud Workload Protection Platform (CWPP) , etc. Antiy has established a closed-loop product system of threat countermeasures based on its threat intelligence and threat detection capabilities, achieving perception, retardation, blocking and presentation of the advanced threats through products such as the Persistent Threat Detection System (PTD), Persistent Threat Analysis System (PTA), Attack Capture System (ACS), and TDS. For web and business security scenarios, Antiy has launched the PTF Next-generation Web Application and API Protection System (WAAP) and SCS Code Security Detection System to help customers shift their security capabilities to the left in the DevOps process. At the same time, it has developed four major kinds of security service: network attack and defense logic deduction, in-depth threat hunting, security threat inspection, and regular security operations. Through the Threat Confrontation Operation Platform (XDR), multiple security products and services are integrated to effectively support the upgrade of comprehensive threat confrontation capabilities.

Antiy provides comprehensive security solutions for clients with high security requirements, including network and information authorities, military forces, ministries, confidential industries, and critical information infrastructure. Antiy has participated in the security work of major national political and social events since 2005 and has won honors such as the Outstanding Contribution Award and Advanced Security Group. Since 2015, Antiy's products and services have provided security support for major spaceflight missions including manned spaceflight, lunar exploration, and space station docking, as well as significant missions such as the maiden flight of large aircraft, escort of main force ships, and Antarctic scientific research. We have received several thank-you letters from relevant departments.

Antiy is a core enabler of the global fundamental security supply chain. Nearly a hundred of the world's leading security and IT enterprises have chosen Antiy as their partner of detection capability. At present, Antiy's threat detection engine provides security detection capabilities for over 1.3 million network devices and over 3 billion smart terminal devices worldwide, which has become a "national-level" engine. As of now, Antiy has filed 1,877 patents in the field of cybersecurity and obtained 936 patents. It has been awarded the title of National Intellectual Property Advantage Enterprise and the 17th (2015) China Patent Excellence Award.

Antiy is an important enterprise node in China emergency response system and has provided early warning and comprehensive emergency response in major security threats and virus outbreaks such as "Code Red", "Dvldr", "Heartbleed", "Bash Shellcode" and "WannaCry". Antiy conducts continuous monitoring and in-depth analysis against dozens of advanced cyberspce threat actors (APT groups) such as "Equation", "White Elephant", "Lotus" and "Greenspot" and their attack actions, assisting customers to form effective protection when the enemy situation is accurately predicted.